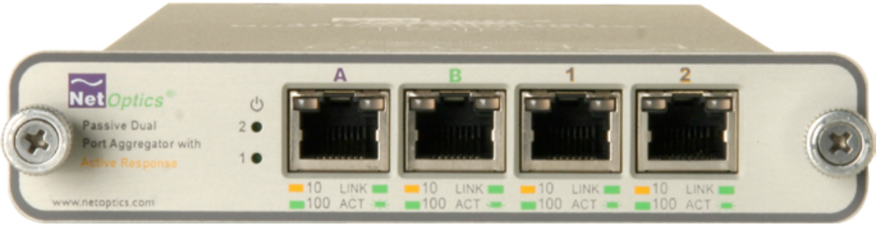
Net Optics®

Installation Guide for

10/100BaseT Port Aggregator Tap

with Active Response

Models PA-CU-AR, PAD-CU-AR



Doc. PUBPACUARU Rev. 1, 06/06

Contents

PLEASE READ THESE LEGAL NOTICES CAREFULLY.

By using a Net Optics Tap you agree to the terms and conditions of usage set forth by Net Optics, Inc.

No licenses, express or implied, are granted with respect to any of the technology described in this manual. Net Optics retains all intellectual property rights associated with the technology described in this manual. This manual is intended to assist with installing Net Optics products into your network.

Trademarks and Copyrights

Additional Information

Net Optics, Inc. reserves the right to make changes in specifications and other information contained in this document without prior notice. Every effort has been made to ensure that the information in this document is accurate.

Introduction

Net Optics 10/100 Dual Port Aggregator Taps with Active Response provide ultra-efficient access to critical links with the option to inject an active response into the network. This pioneering technology enables any two devices to simultaneously monitor a full-duplex link - using only one NIC per device.

Typically, full-duplex monitoring with a network tap requires two NICs (or a dual channel NIC) – one interface for each side of the tapped full-duplex connection. The Dual Port Aggregator Tap combines and regenerates these streams, sending all aggregated data out two separate passive monitoring ports. The best part of this innovation is the onboard memory to make sure traffic isn’t dropped during bursts.

Response Ready

When active responses to network events are required, the first monitoring port can be changed to an Active Response Port using a hardware switch. The Active Response Port buffers and transmits into the network link any type of Ethernet packet, from a simple TCP reset to ICMP messages. The Active Response Port can be easily switched back to passive monitoring via the hardware switch.

The combination of active response capability and passive monitoring in the Tap reduces the number of devices and network ports required for active response functionality.

Buffering Prevents Lost Data

The Dual Port Aggregator Tap with Active Response is designed to handle the combined traffic of a single full-duplex link. Normally, the traffic should be below the receiving capacity of the NIC, that is, less than 10 or 100 Mbps.

When the traffic queue exceeds the capacity of the NIC, the Tap buffers the overflow of up to one megabyte per side of the full-duplex connection. For your convenience, the buffers clear automatically when the traffic volume falls below the receiving capacity of the NIC. For example, if there is a traffic burst and a tap connected to a 100 Mbps network port on a monitoring device is now receiving 140 Mbps of traffic, the Tap buffers data until the burst is over. The Tap then sends the buffered data to the monitoring device until the buffer is cleared.

Simple to Deploy

Net Optics' Dual Port Aggregator Tap with Active Response is a simple plug-and-play solution addressing the fact that many monitoring systems, including

most software based solutions, only offer a single channel NIC, limiting full-duplex visibility. While adding a second NIC can help maintain data integrity and visibility, there is a tradeoff in flexibility and ease-of-use. An operating system and NICs that enable binding are often required to achieve the same functionality as the Dual Port Aggregator Tap. In contrast, the Dual Port Aggregator Tap requires no additional components or configuration on the monitoring devices.

All network and monitoring cables required for plug-and-play deployment are included with the 10/100BaseT Dual Port Aggregator Tap w/Active Response.

Better than Span Ports

In the past, span ports were occasionally used to aggregate tapped traffic. However, in addition to other shortcomings of span port monitoring, span ports support very limited buffering and can simply drop data during bursts. The generous buffers of the Dual Port Aggregator Tap prevent data loss in these conditions.

Security and Visibility

Without an IP address, monitoring devices are isolated from the network, dramatically reducing their exposure to attacks. However, the monitoring device connected to the Tap still sees all full-duplex traffic as if it were in-line, including Layer 1 and Layer 2 errors.

Reliability

For extra uptime protection, Net Optics Taps offer redundant power connections. Should the primary power source fail, the Tap automatically switches to the backup power source. Power LEDs on the front of the Tap indicate the current power source.

Key Features

Passive, Secure Technology

- Supports full-duplex monitoring with a single NIC, increasing monitoring efficiency
- Regeneration Tap technology enables two devices to simultaneously monitor all aggregated traffic – using only one NIC per device
- One megabyte of memory for each side of the full-duplex link (two megabytes memory, total) prevents data loss during excessive traffic loads
- Provides complete full-duplex visibility at 10 or 100 Mbps without data stream interference or introducing a point of failure
- No IP address is needed for the Tap or monitoring device, enhancing monitoring security
- Compatible with Mid-Span Power over Ethernet (PoE) applications
- Redundant power ensures monitoring uptime
- Fully RoHS compliant

Enhanced, Efficient Monitoring

- Active response capability increases Tap-based monitoring flexibility and efficiency
- Hardware switch provides a secure transition between passive mode (transmit only) and active mode (transmit/receive) for the Active Response Port

Ease of Use

- LED indicators show redundant power, speed, link, and activity status
- DIP switches select auto-negotiation or fixed speed and duplexing settings for the Tap
- Front-mounted connectors support easy installation and operation
- Silk-screened application diagram illustrates all connections for easy deployment
- Optional 19-inch rack frames hold up to three Taps
- Tested and compatible with all major manufacturers' monitoring devices, including protocol analyzers, probes, and intrusion detection/prevention systems

Support

- Net Optics offers free technical throughout the lifetime of your purchase. Our technical support team is available from 8 am to 5 pm Pacific Time, Monday through Friday at +1 (408) 737-7777 and via email at ts-support@netoptics.com. FAQs are also available on Net Optics website at www.netoptics.com.

Unpacking and Inspection

Carefully unpack the 10/100 Port Aggregator Tap w/Active Response and check for damaged or missing parts. The Tap ships with the following:

- 10/100 Port Aggregator Tap w/Active Response
- Two power supplies
- Two network cables
- One or two monitor cables
- Installation Guide

You may have also ordered a one rack unit panel for mounting three Taps and an extended warranty. Carefully check the packing slip against parts received. If any part is missing or damaged, contact Net Optics' Customer Service immediately.

Product Diagrams

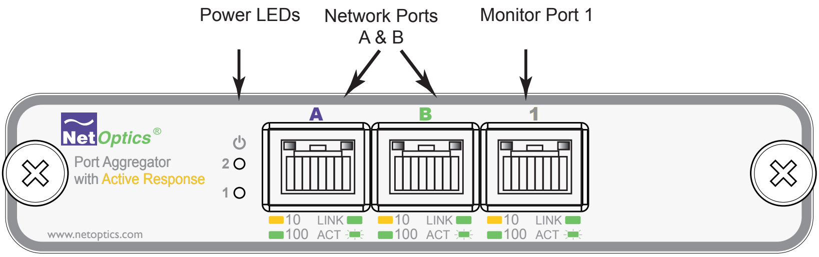


Figure 1: PA-CU-AR Front Panel

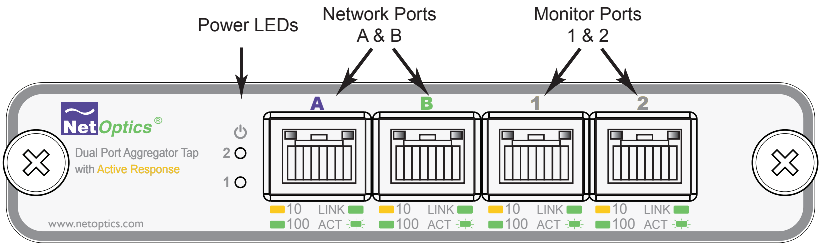


Figure 2: PAD-CU-AR Front Panel

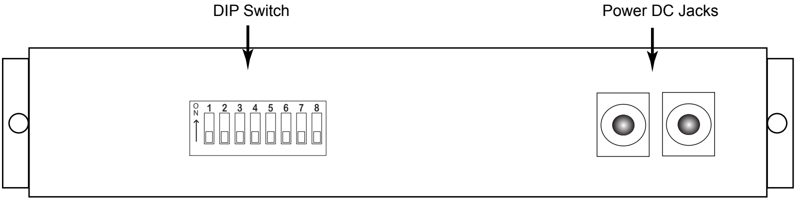


Figure 3: Rear Panel

LED Indicators

- **PWR 1/ PWR 2:** Main and Redundant Power. If the Tap is deployed with both power supplies, both LEDs will illuminate when the Tap is plugged in. If an LED is off, this indicates that the corresponding power supply is not functioning.

Additional Port Aggregator Tap LEDs are located in the upper left and right hand corners of the RJ45 connectors for Port A, Port B, Port 1 and Port 2 (PAD-CU-AR only).

- **10/100 Indicator:** If the Port is set to 10 Mbps, the LED illuminates orange. If the Port is set to 100 Mbps, the LED illuminates green.
- **Link/Activity Indicators:** If a good link is established, the LED illuminates a steady green. If there is current activity on this link, the LED flashes.

Application Diagrams: Memory Operation

All traffic that passes through the Tap is sent to the monitoring device NIC on a first-in, first-out basis, including traffic that is temporarily stored in memory. (If two packets enter at the same time then one packet is processed while the other is stored briefly in memory, preventing collisions.)

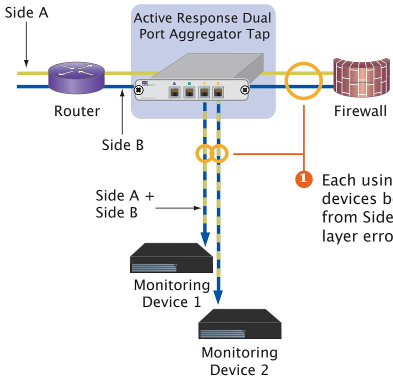
When there is a burst of data, traffic in excess of the NIC's capacity is sent to the Tap's memory. Up to one megabyte of data per side of the full-duplex stream can be stored in memory. Memory continues to fill until its capacity is reached, or the burst ends – whichever comes first.

In both cases, the Tap applies a first-in, first out procedure, processing stored data before new data from the link. If memory fills before the burst ends, the memory stays filled as the stored data is processed – data that leaves the buffer is immediately replaced. If the burst ends before the memory fills, memory clears until the full megabyte of capacity is available, or until another burst in excess of the NIC's capacity requires additional memory.

The following three diagrams illustrate a simple example of a 100 Mbps NIC moving from 80 percent utilization, to 140 percent utilization, then back to 80 percent utilization. If you have PA-CU-AR model, there is only one monitor port.

State 1: Side A + Side B is less than or equal to 100% of the NIC's receive capacity.

Example: On a 100 Mbps link, Side A is at 30 Mbps and Side B is at 50 Mbps. The NIC receives 80 Mbps of traffic (80% utilization), so no memory is required for the monitoring device NIC to process all full-duplex traffic.

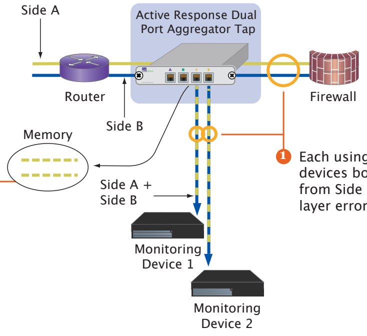


1 Each using a single NIC, the monitoring devices both receive all combined traffic from Side A and Side B, including physical layer errors.

Figure 4: 80% Utilization

State 2: Side A + Side B becomes greater than 100% of the NIC's receive capacity.

Example: There is a burst of traffic, so Side A is now at 90 Mbps while Side B remains at 50 Mbps. The NIC's utilization is at 140%, requiring the use of memory to help prevent data loss.



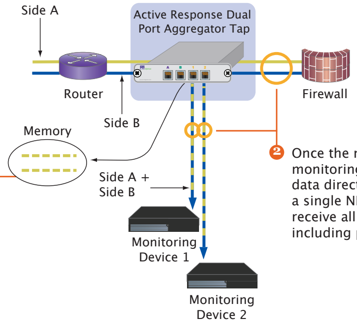
2 The extra 40 Mbps of traffic is stored in the 1 megabyte buffer for Port A. Memory continues to fill until the 1 megabyte capacity is reached, or the burst ends. (A separate 1 megabyte buffer is also available to handle a burst on Port B.)

1 Each using a single NIC, the monitoring devices both receive all combined traffic from Side A and Side B, including physical layer errors.

Figure 5: 140% Utilization

State 3: Side A + Side B is once again less than 100% of the NIC's receive capacity.

Example: On a 100 Mbps link, Side A is again at 30 Mbps and Side B remains at 50 Mbps. The NIC's utilization is again at 80%.



1 The Tap applies a first-in, first-out process to all packets. Once the burst has ended and the NIC's utilization is again below 100 percent, the Tap first processes the packets that were stored in memory. As long as the NIC's utilization remains below 100 percent, this process continues uninterrupted until the memory clears.

2 Once the memory has cleared, each monitoring device begins receiving new data directly from the link. Each using a single NIC, both monitoring devices receive all traffic from Side A and Side B, including physical layer errors.

Figure 6: Return to 80% Utilization

Cabling Guidelines

Use straight-through cable to connect the Tap Ports to a Router or NIC. Use cross-over cable to connect the Tap Ports to Switches and Hubs. The Tap Ports Transmit on Pins 3 & 6 and Receive on Pins 1 & 2.

Note:

You must ensure that both Network Ports A and B match speed and duplex settings on your network devices.

Connecting to the Network

1. Connect Network Port A to the appropriate network device following the cabling guidelines above.

2. Connect Network Port B to the appropriate network device following the cabling guidelines above.

3. Verify that the Tap Network Ports are cabled in-line between two devices.

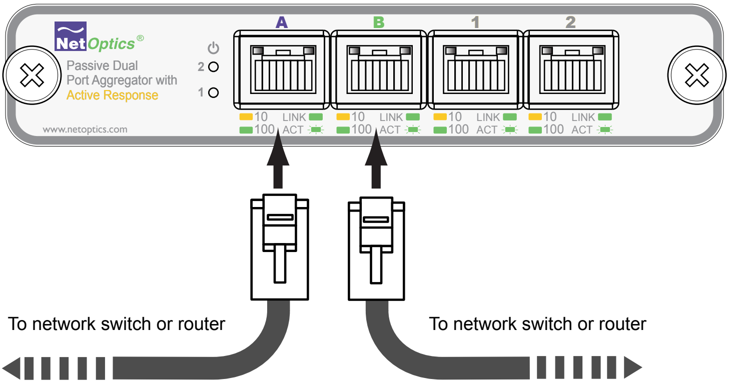


Figure 7: Connecting to the Network

Connecting to the Monitoring Device(s)

1. Supply power to the Tap using the power supplies included with the unit. Two power supplies are included. The use of the second redundant power supply is optional.

Note:

The second power supply is available to support the flow of traffic to the monitoring device, in the event that the first power supply becomes unavailable. If the first power supply is unavailable, the second power supply will supply all power for the Tap. Even if no power is available to the passive Tap, network traffic flows uninterrupted.

2. Verify that the Power LEDs illuminate. PWR 1 illuminates when the first power supply is in use, and PWR 2 illuminates when the second power supply is in use. Both power supplies can be plugged into the Tap at the same time.

3. Connect Monitoring Port 1 to the appropriate port on the monitoring device using a CAT5 RJ45 straight-through cable to monitor the full-duplex link.

4. If you are installing model PAD-CU-AR, connect Monitoring Port 2 to the appropriate port on the monitoring device using a CAT5 RJ45 straight-through cable to monitor the full-duplex link.

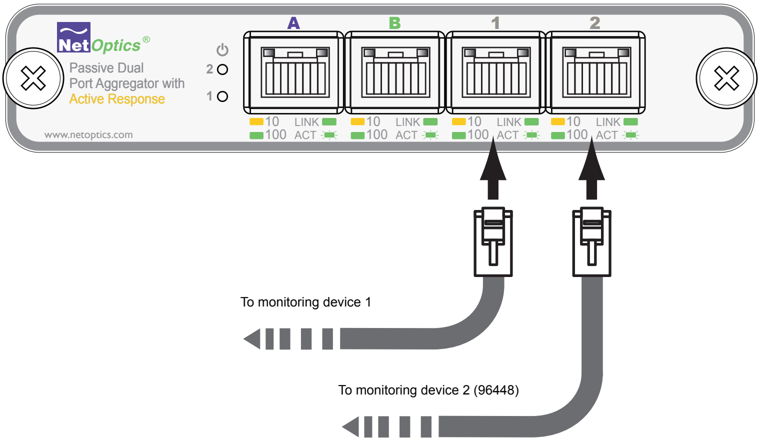
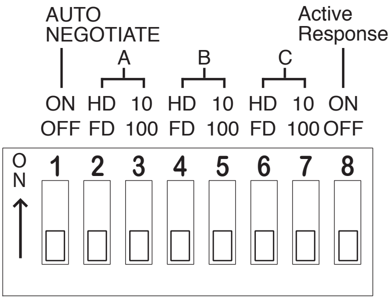


Figure 8: Connecting to Monitoring Device(s)

DIP Switch Settings

Switch	Function	Description
1	Turns Auto-negotiation ON or OFF. Factory default setting is Auto-negotiation.	If turned ON, ports A, B, and C/D automatically negotiate the links. Positions 2 thru 8 are inactive. To manually configure ports A, B, and C/D, turn switch to the OFF position. Positions 2 thru 8 are active.
2	Set Port A Duplex	ON for Half-Duplex; turn OFF for Full-Duplex
3	Set Port A Speed	ON for 10 Mbps; turn OFF for 100 Mbps
4	Set Port B Duplex	ON for Half-Duplex; turn OFF for Full-Duplex
5	Set Port B Speed	ON for 10 Mbps; turn OFF for 100 Mbps
6	Set Port 1 (and 2) Duplex	ON for Half-Duplex; turn OFF for Full-Duplex
7	Set Port 1 (and 2) Speed	ON for 10 Mbps; turn OFF for 100 Mbps
8	Active Response	Turns Active Response ON or OFF



NOTE: To activate, push buttons UP.
(This diagram shows all segments
in the OFF position)

Figure 9: DIP Switch Settings

Active Response Tap FAQs

Q: What types of active responses are supported?

A: With an Active Response Dual Port Aggregator Tap, an administrator can transmit any type of Ethernet packet back into the original link, supporting all common types of active responses generated by intrusion detection systems, and by intrusion prevention systems deployed in passive mode. The most common response types are TCP resets, and firewall rule changes. While the Tap can support both types of responses, we advocate extreme caution in dynamically updating firewall rules due to the risk of disabling network services. Because most firewalls are managed out-of-band, however, it is unlikely that the Regeneration Tap will be part of a rule change scenario.

Q: How are collisions avoided when active responses are transmitted back into the original link?

A: On each side of the full-duplex link, there is a small buffer for traffic arriving from the network, and another small buffer for active response traffic arriving from the monitoring device. Traffic is released from this buffer pair on a first-in, first-out basis. If both sides of the buffer are empty and a packet originating from the monitoring device and a packet originating from the network arrive at the same time, priority is given to the network packet.

Active Response Tap FAQs (Continued)

Q: How much bandwidth is available on the Active Response Port?

A: The average amount of bandwidth for active responses is determined by the average available capacity on the link. For example, on a 100 Mbps full-duplex link, if transmission from device A to device B averages 30 Mbps, and transmission from device B to device A averages at 50 Mbps, then there is an average capacity on the first side for 70 Mbps, and on the second side for up to 50 Mbps of active response traffic.

At any particular point in time, actual capacity is determined by the size of the packets being transmitted and the gap between these packets. On a standard link with 64-byte network and active response traffic, the capacity at any point in time will be very close to the average capacity. (We do not recommend using the Tap on links with jumbo packets as these large – up to 9K – packets can fill the buffer and impact performance.)

As the most common use for the Tap will be to inject TCP resets, which are standard 64-byte packets, it is unlikely that the transmissions from either side of the Active Response Port will exceed 10 Mbps, even if many sessions are terminated in a short time frame. In our internal testing, we have therefore focused on Active Response Port performance at up to 10 Mbps.

Q: Does Active Response Port require the connected monitoring device to have an IP address?

A: Yes, the connected monitoring device is required to have a MAC and IP address when the Active Response Port is operating in active mode. These are not required when this Port is set to passive mode. The Tap itself never has a MAC or IP address, regardless of how the Active Response Port is set.

Specifications

Environment

Operating Temperature: 0°C to 55°C
Storage Temperature: -10°C to 70°C
Relative Humidity: 10% min, 95% max, non-condensing

Power

Power Supply Input: 100-240VAC, 0.5A, 47-63Hz
Output: 12V, 1.5A

Mechanical

Dimensions: 1.125” high x 9.125” deep x 4.5” wide

Cable Interface

Copper Cable Type: 22-24 AWG unshielded twisted pair cable, CAT5/CAT5e
Link Distance Supported: 100 meters

Connectors

(2) RJ45, 8-pin connectors (network ports)
(1) RJ45, 8-pin connector (PA-CU-AR monitor port)
(2) RJ45, 8-pin connectors (PAD-CU-AR monitor ports)

Certifications

Fully RoHS compliant

Limitations on Warranty and Liability

Net Optics offers a limited warranty for all its products. IN NO EVENT SHALL NET OPTICS, INC. BE LIABLE FOR ANY DAMAGES INCURRED BY THE USE OF THE PRODUCTS (INCLUDING BOTH HARDWARE AND SOFTWARE) DESCRIBED IN THIS MANUAL, OR BY ANY DEFECT OR INACCURACY IN THIS MANUAL ITSELF. THIS INCLUDES BUT IS NOT LIMITED TO LOST PROFITS, LOST SAVINGS, AND ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT, even if Net Optics has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Net Optics, Inc. warrants this Tap to be in good working order for a period of ONE YEAR from the date of purchase from Net Optics or an authorized Net Optics reseller.

Should the unit fail anytime during the said ONE YEAR period, Net Optics will, at its discretion, repair or replace the product. This warranty is limited to defects in workmanship and materials and does not cover damage from accident, disaster, misuse, abuse or unauthorized modifications.

If you have a problem and require service, please call the number listed at the end of this section and speak with our technical service personnel. They may provide you with an RMA number, which must accompany any returned product. Return the product in its original shipping container (or equivalent) insured and with proof of purchase.

Additional Information

Net Optics, Inc. reserves the right to make changes in specifications and other information contained in this document without prior notice. Every effort has been made to ensure that the information in this document is accurate. Net Optics is not responsible for typographical errors.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, EXPRESS OR IMPLIED. No Net Optics reseller, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

Net Optics is always open to any comments or suggestions you may have about its products and/or this manual.

Send correspondence to
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054 USA
Telephone: +1 (408) 737-7777
Fax: +1 (408) 745-7719
Email: info@netoptics.com/Internet: www.netoptics.com

www.netoptics.com